Block Cipher Modes of Operation

Presented By:
Khushi Patel,
Assistant Professor,
Department of Computer Engineering
DEPSTAR, CHARUSAT

Abstract

- We will discuss
  - How to use a block cipher?
  - Various modes of operations for block cipher

How to use a block cipher?

- Block ciphers encrypt fixed-size blocks
  - e.g. DES encrypts 64-bit blocks
- We need some way to encrypt a message of arbitrary length
  - e.g. a message of 1000 bytes
- NIST defines several ways to do it
  - called **modes of operation**

Modes of Operations

Five Modes of Operation

- Electronic codebook mode (ECB)
- Cipher block chaining mode (CBC) – most popular
- Output feedback mode (OFB)
- Cipher feedback mode (CFB)
- Counter mode (CTR)

Message Padding

- The plaintext message is broken into blocks, P_1, P_2, P_3, ...
- The last block may be short of a whole block and needs padding.
- Possible padding:
  - Known non-data values (e.g. nulls)
  - Or a number indicating the size of the pad
  - Or a number indicating the size of the plaintext
  - The last two schemes may require an extra block.

Electronic Code Book (ECB)

- The plaintext is broken into blocks, P_1, P_2, P_3, ...
- Each block is encrypted independently:

  $$C_i = E_K(P_i)$$

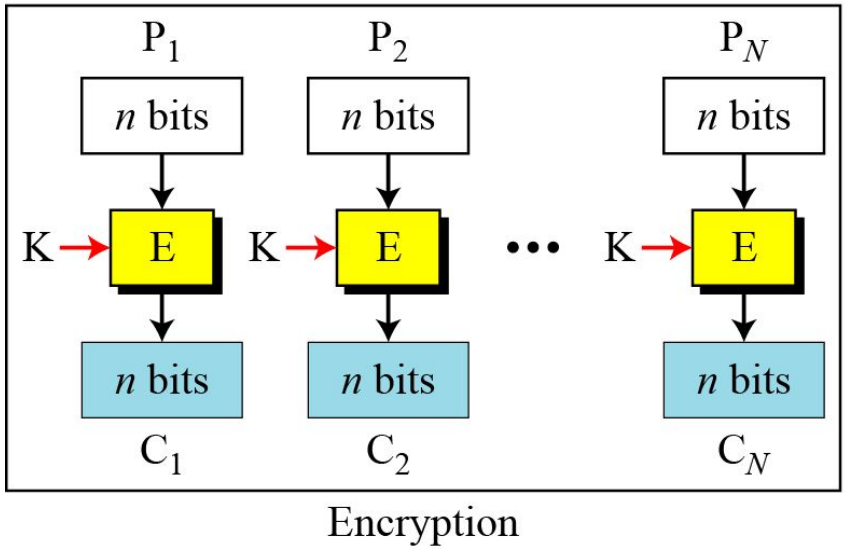
- For a given key, this mode behaves like we have a gigantic codebook, in which each plaintext block has an entry, hence the name Electronic Code Book
- Decryption:

  $P_i = D_k(C_i)$

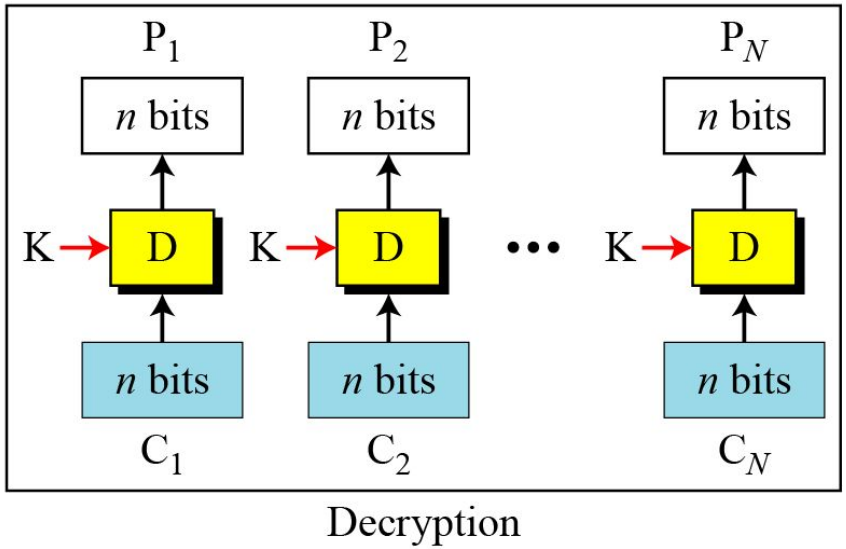
$$P_i = D_k(C_i) = D_k(E_K(P_i)) = P_i$$

Continue..

E: Encryption D: Decryption
P_i: Plaintext block i C_i: Ciphertext block i
K: Secret key



Encryption



Decryption

Remarks on ECB

- Strength: it's simple.
- Weakness:
  - Repetitive information contained in the plaintext may show in the ciphertext, if aligned with blocks.
  - If the same message (e.g., an SSN) is encrypted (with the same key) and sent twice, their ciphertexts are the same.
- Typical application: secure transmission of short pieces of information (e.g. a temporary encryption key)

Cipher Block Chaining (CBC)

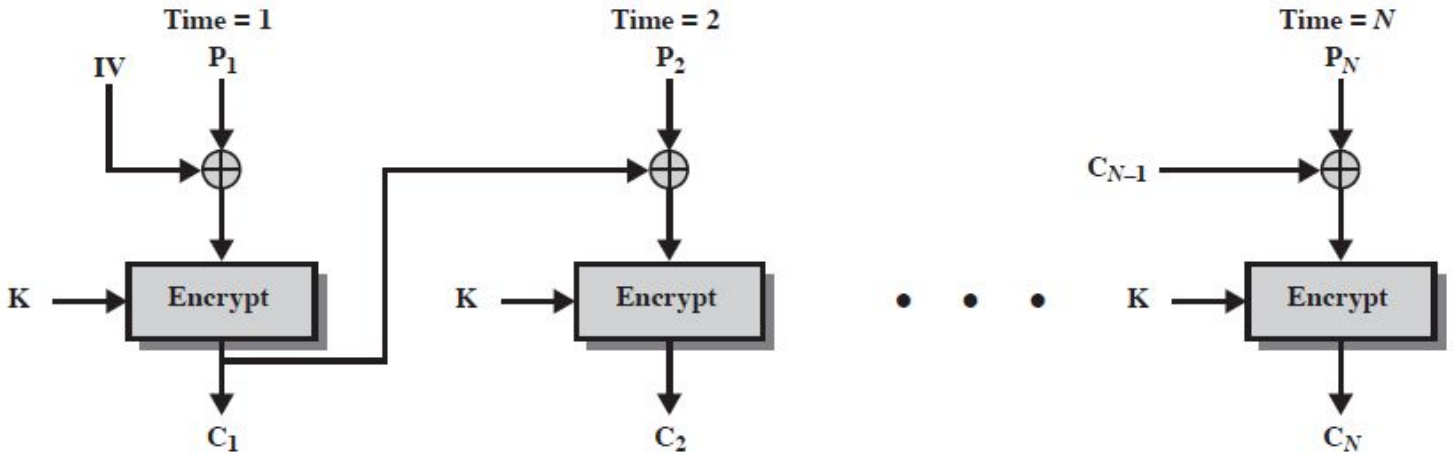
- The plaintext is broken into blocks: $P_1,\ P_2,\ P_3,\ \ldots$
- Each plaintext block is XORed (chained) with the previous ciphertext block before encryption (hence the name):

$$C_i = \mathrm{E}_K\left(C_{i-1} \oplus P_i\right)$$

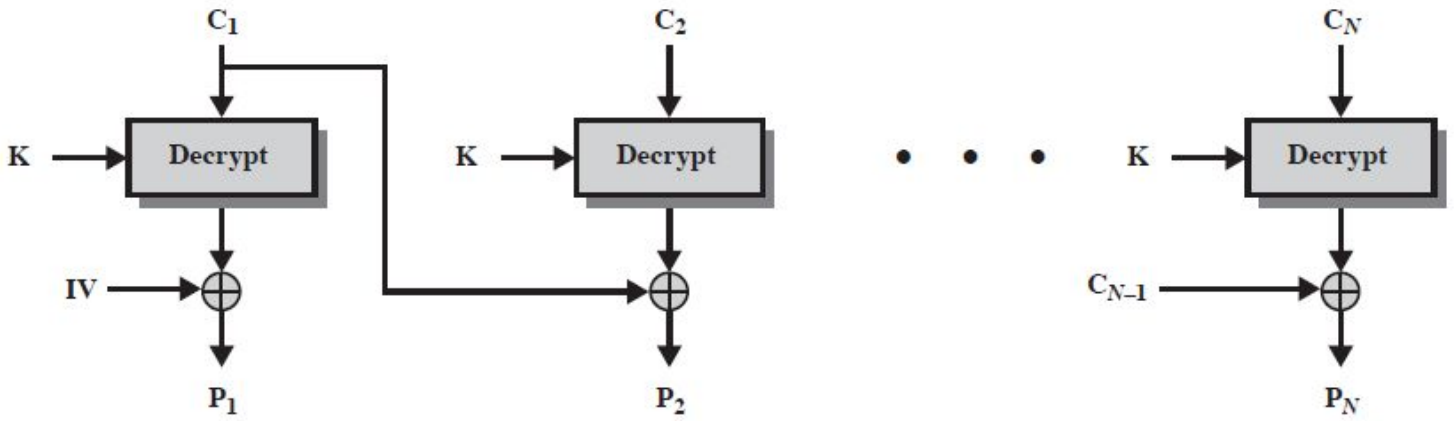
$$C_0 = \mathrm{IV}$$

- Use an Initial Vector (IV) to start the process.
- Decryption: $P_i = C_{i-1} \oplus \mathrm{D}_K(C_i)$
- Application: general block-oriented transmission.

Cipher Block Chaining (CBC)



(a) Encryption



(b) Decryption

Remarks on CBC

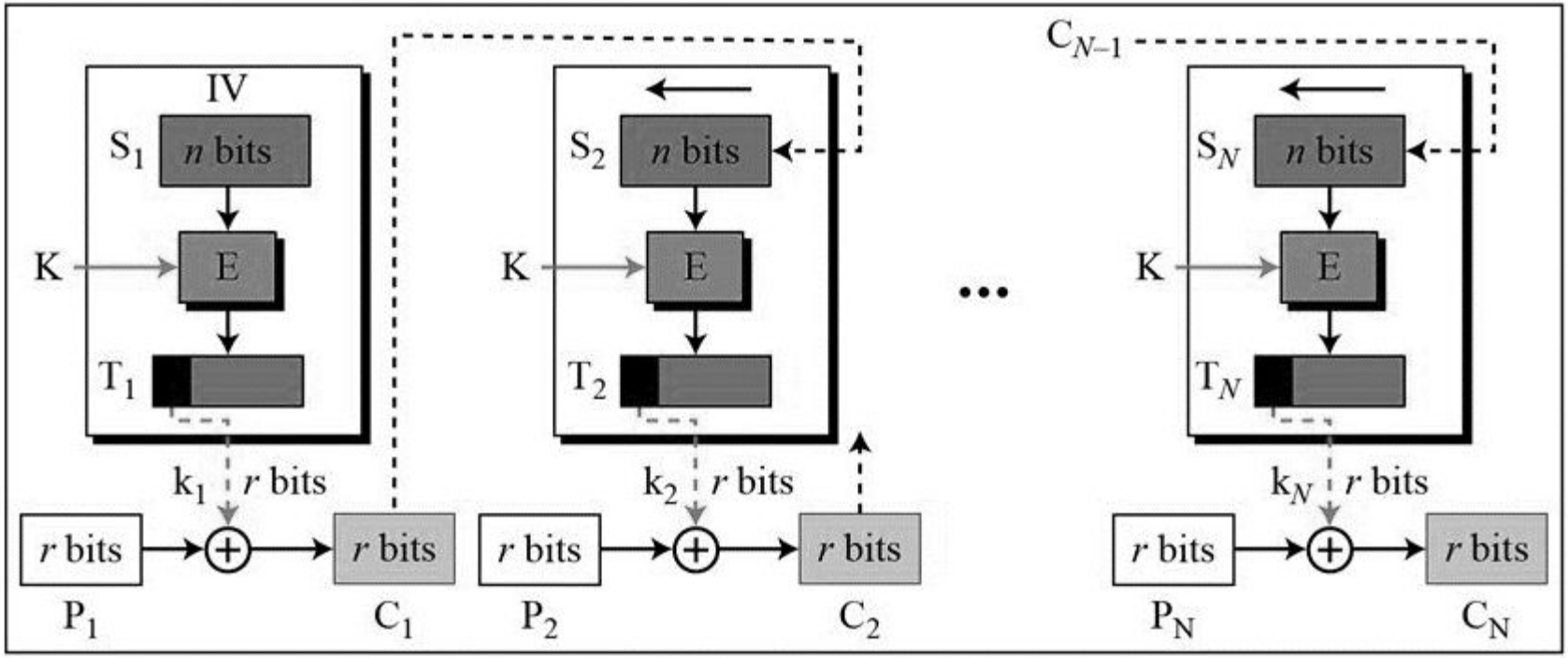
- The encryption of a block depends on the current and **all** blocks before it.
- So, repeated plaintext blocks are encrypted differently.
- Initialization Vector (IV)
  - Must be known to both the sender & receiver
  - Typically, IV is either a fixed value or is sent encrypted in ECB mode before the rest of ciphertext.

Cipher Feedback Mode

E : Encryption
P_i: Plaintext block *i*
K: Secret key

D : Decryption
C_i: Ciphertext block *i*
IV: Initial vector (S_1)

S_i: Shift register
T_i: Temporary register



Encryption

continue

- Encryption:

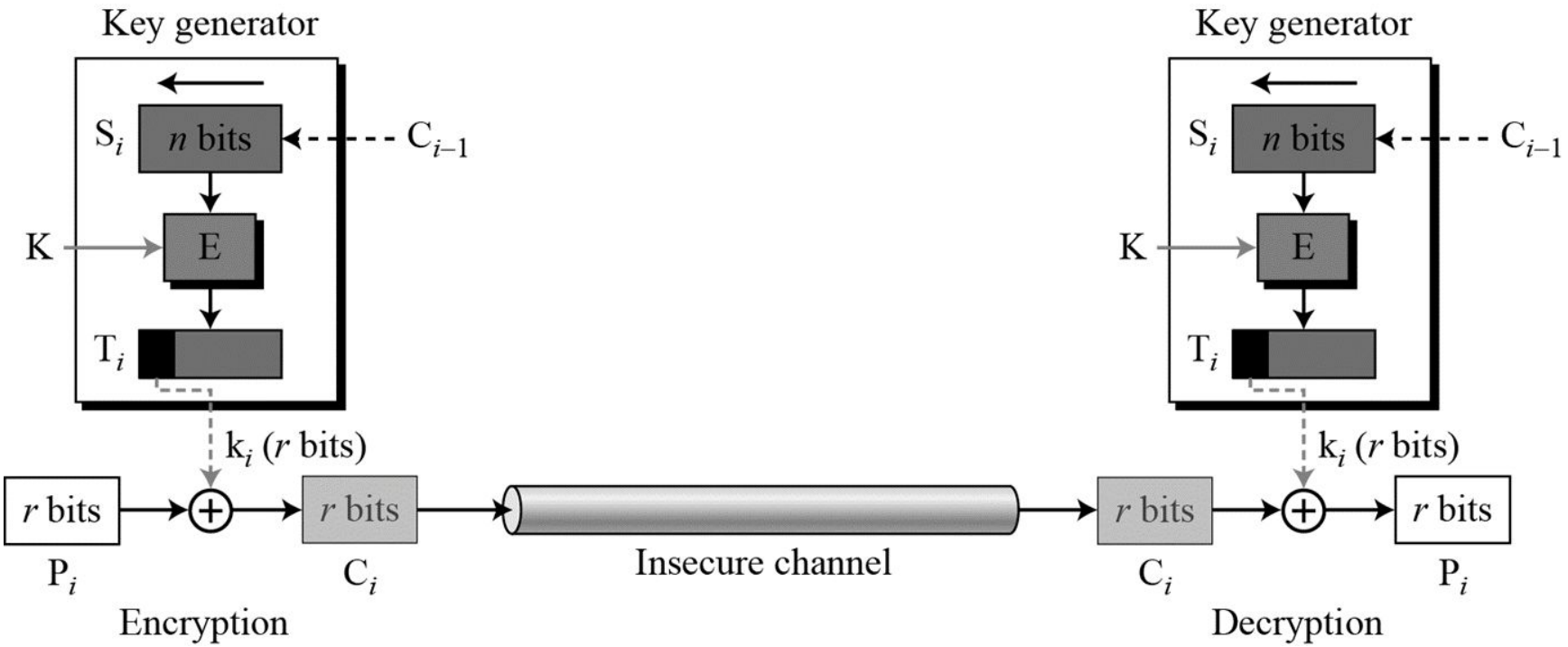
  $S_0 = IV$

  $C_i = P_i \oplus \text{SelectLeft}_r \{ E_k [\text{shiftLeft}_r (S_{i-1}) \mid C_{i-1}] \}$

- Decryption:

  $P_i = C_i \oplus \text{SelectLeft}_r \{ E_k [\text{shiftLeft}_r (S_{i-1}) \mid C_{i-1}] \}$

CFB as a Stream Cipher



Remark on CFB

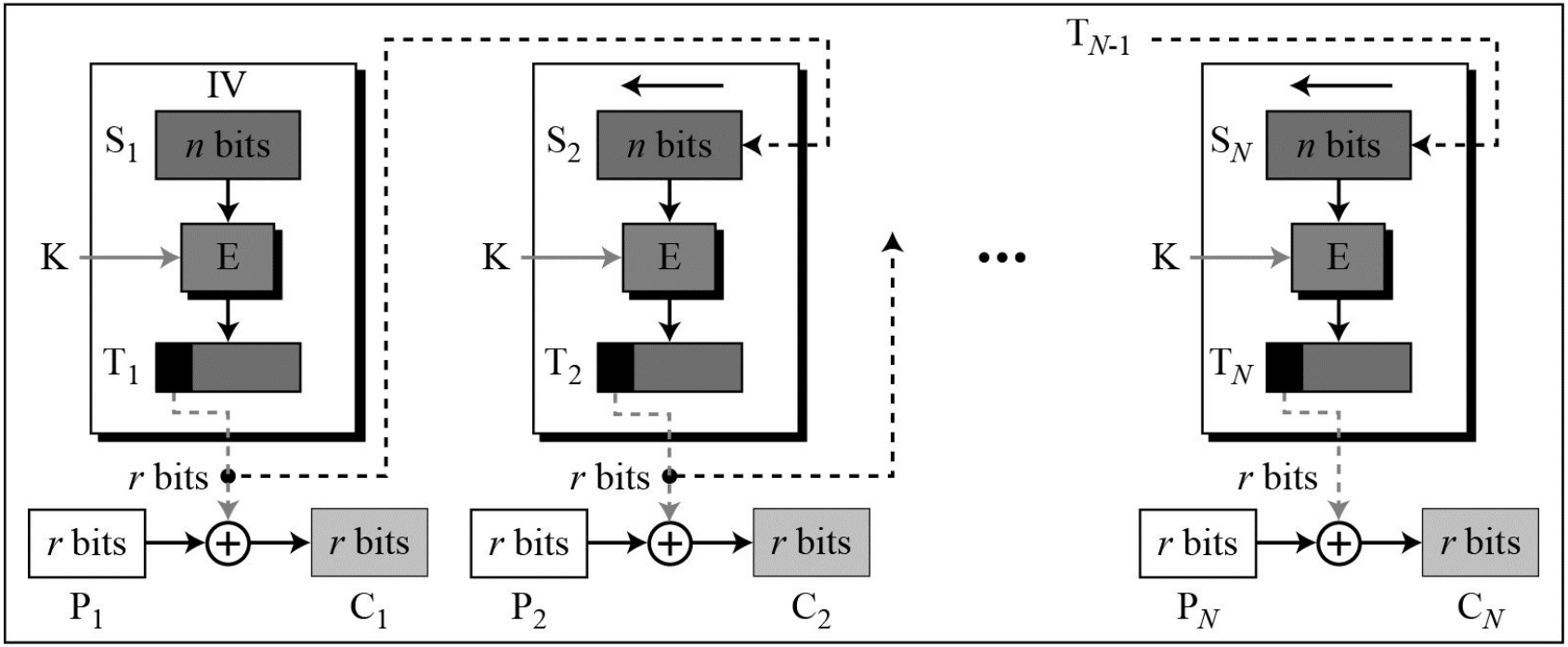
- The block cipher is used as a stream cipher.
- Appropriate when data arrives in bits/bytes.
- s can be any value; a common value is s = 8.
- A ciphertext segment depends on the current and all preceding plaintext segments.
- A corrupted ciphertext segment during transmission will affect the current and next several plaintext segments.

Output Feedback (OFB) Mode

E : Encryption
P_i: Plaintext block i
K: Secret key

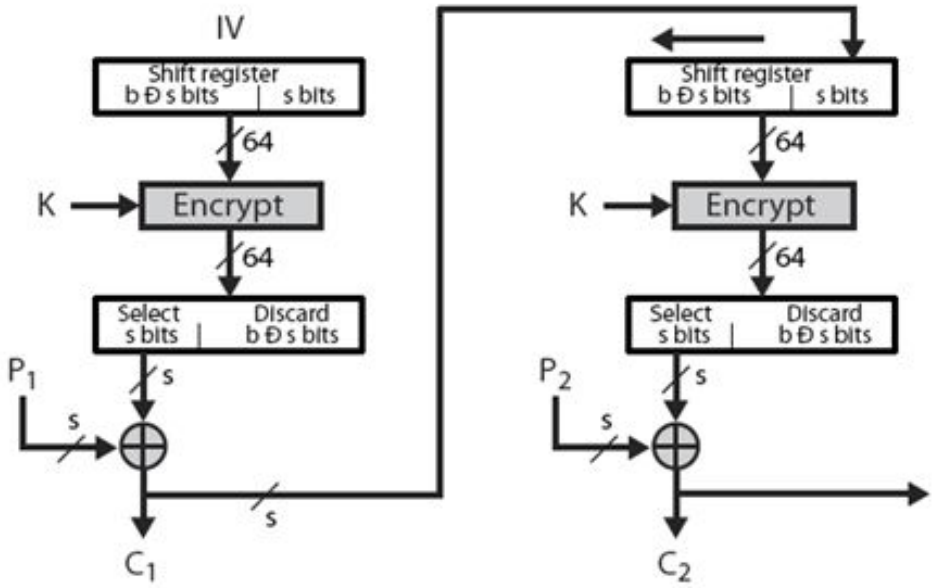
D : Decryption
C_i: Ciphertext block i
IV: Initial vector (S_1)

S_i: Shift register
T_i: Temporary register

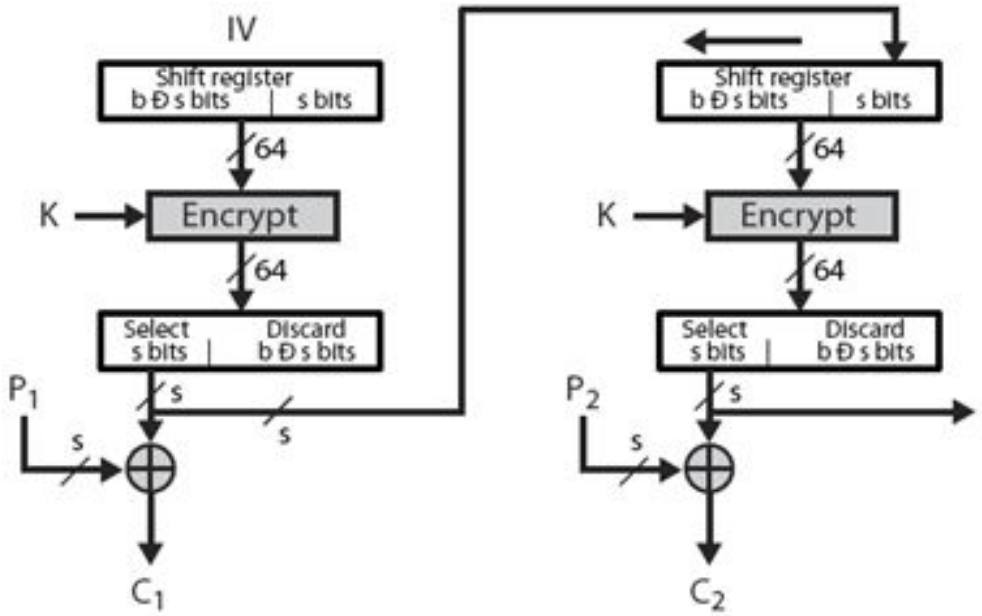


Encryption

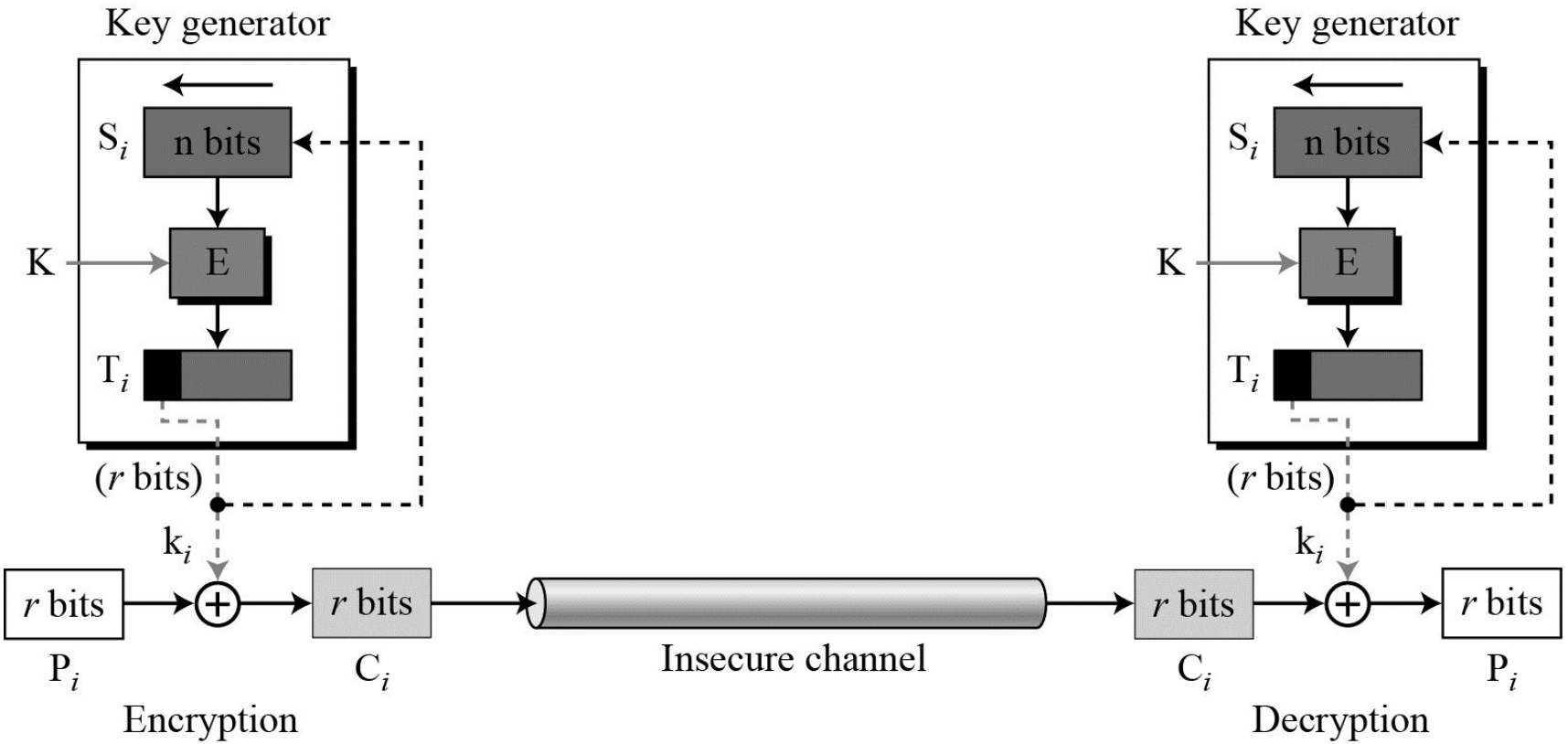
Cipher Feedback



Output Feedback



OFB as a Stream Cipher



Remark on OFB

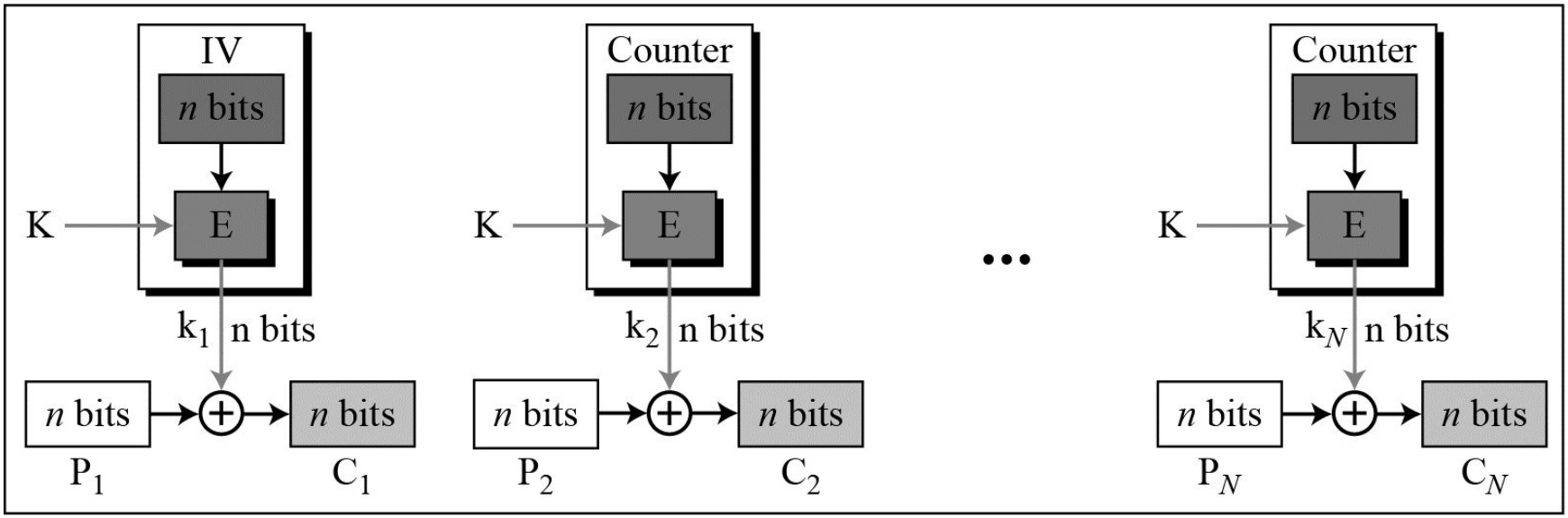
- The block cipher is used as a stream cipher.
- Appropriate when data arrives in bits/bytes.
- Advantage:
  - more resistant to transmission errors; a bit error in a ciphertext segment affects only the decryption of that segment.
- Disadvantage:
  - Cannot recover from lost ciphertext segments; if a ciphertext segment is lost, all following segments will be decrypted incorrectly (if the receiver is not aware of the segment loss).
- IV should be generated randomly each time and sent with the ciphertext.

Counter Mode (CTR)

E : Encryption
P_i : Plaintext block *i*
K : Secret key

IV: Initialization vector
C_i : Ciphertext block *i*
k_i : Encryption key *i*

The counter is incremented for each block.



Encryption

Remark on CTR

- Strengthes:
  - Needs only the encryption algorithm
  - Fast encryption/decryption; blocks can be processed (encrypted or decrypted) in parallel; good for high speed links
  - Random access to encrypted data blocks
- IV should not be reused.

Bifurcation

- Although Five modes of operations enable the use of block ciphers for encipherment of messages or files in large units(ECB,CBC, CTR) and small units (CFB and OFB).

comparision

Operation Mode	Description	Type of Result	Data Unit Size
ECB	Each n bit block is encrypted independently with the same cipher key	Block cipher	N
CBC	Same as ECB, but each block is first X-ORed with the previous ciphertext	Block cipher	N
CFB	Each r bit block is X-ORed with r-bit key, which is part of previous cipher text	Stream cipher	R<=N
OFB	Same as CFB, but the shift register is updated by the previous r bit key	Stream cipher	R<=N
CTR	Same as OFB, but a counter is used instead of a shift register	Stream cipher	N

Questions??

- Divide five modes of operation into two groups: those that use the encryption and decryption function of underlying cipher (For example, DES and AES) and those that use only the encryption function.
- Divide the five modes of operation into two groups: those that need padding and those that do not.
- Divide the five modes of operation into two groups: those that use the same key for the encipherment of all blocks and those that use a key stream for encipherment of blocks.

References

- Cryptography and network security – Behrouz a forouzan, debdeep mukhopadhyay

Thank You